Cybersecurity: Europese Unie initiatieven voor een intrinsiek grensoverschrijdend fenomeen

Lodder, A.R.; Toet, J.

published in
Tijdschrift voor Internetrecht
2013

document version
Publisher's PDF, also known as Version of record

Cybersecurity: Europese Unie initiatieven voor een intrinsiek grensoverschrijdend fenomeen

Arno R. Lodder en Joeri Toet[*]

Het ontstaan van de Europese Unie valt samen met de opkomst van het internet. Net als de Europese Unie heeft het internet de afgelopen twintig jaar veel goeds gebracht, maar zijn er ook mindere kanten. Cybersecurity richt zich op de dreigingen die de veiligheid op internet aantasten. De Europese Unie erkent het belang van het goed functioneren van het internet en heeft recent enkele initiatieven ondernomen om de veiligheid op internet te versterken. In deze bijdrage wordt de achtergrond van cybersecurity geschetst en onder andere ingegaan op de Richtlijn 2013/40/EU inzake aanvallen op informatiesystemen, het in 2013 opgerichte Europese Cybersecurity Centrum en de begin 2013 voorgestelde richtlijn Netwerk- en Informatiebeveiliging.

Inleiding

De term *diensten van de informatiemaatschappij*[1] wordt sinds eind jaren negentig binnen de Europese Unie gebruikt om internetdiensten mee aan te duiden. Dit illustreert de centrale rol die internet in de informatiemaatschappij inneemt. Om die reden is het streven naar online veiligheid een belangrijk thema, populair aangeduid als cybersecurity. De dreigingen op internet zijn talrijk en komen van een groot aantal, qua achtergrond zeer diverse actoren (overheden, criminelen, activisten, etc.). Het is daarom niet eenvoudig om goede regelgeving te ontwerpen en adequate maatregelen te treffen. Een vraag die vanuit de normering leidend moet zijn, is:

> Verbeteren juridische maatregelen het niveau van informatiebeveiliging en helpen deze de gevolgen van een inbreuk beperken?

In deze bijdrage zullen we mede aan de hand van deze vraag aangeven hoe de Europese Unie invulling aan het dossier cybersecurity geeft. Eerst zullen we de achtergrond van cybersecurity schetsen, zowel in historisch perspectief als tegen de achtergrond van relevante wettelijke normen. Vervolgens gaan wij in op initiatieven van de Europese Unie op het terrein van cybersecurity en zullen daarbij vooral aandacht besteden aan de begin 2013 voorgestelde Richtlijn informatiebeveiliging, voluit de Richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.[2]

Achtergrond

Wat is cybersecurity?

Het thema 'cybersecurity' houdt de gemoederen bezig. Iedereen lijkt erover mee te kunnen praten, maar wat moet er onder verstaan worden en wat kunnen we ertoe ondernemen? Een eenduidige definitie van de term cybersecurity is er niet. Dit stelt ook ENISA vrij recentelijk nog vast in haar beschouwing van verschillende Europese cybersecurity strategieën.[3] In de Nationale Cybersecuritystrategie wordt cybersecurity als volgt gedefinieerd:

> 'Cybersecurity is het vrij zijn van gevaar of schade veroorzaakt door storing of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.'

In deze definitie komt het verband met informatiebeveiliging nadrukkelijk naar voren door de referenties naar het bekende CIA principe. *Confidentiality* (vertrouwelijkheid), *Integrity* (integriteit) en *Availability* (beschikbaarheid). Deze drie begrippen vormen de kern van informatiebeveiliging, soms aangevuld met *authenticity* (authenticiteit) en *reliability* (betrouwbaarheid). Wat ook opvalt is het gebruik van de term ICT: Informatie- en Communicatietechnologie beperkt zich niet enkel tot internet, terwijl de prefix 'cyber' doorgaans wordt gereserveerd voor met internet samenhangende termen als cyberspace, cybercrime en cyberpesten.
De terminologische verwarring is groot: zo zijn er mensen die cybersecurity te pas en te onpas gebruikt vinden en liever de algemene term informatiebeveiliging hanteren voor met internet samenhangende veiligheid en beveiliging, an-

---

* Arno R. Lodder is hoogleraar Internet Governance and Regulation aan de Vrije Universiteit Amsterdam, afdeling Transnational Legal studies. Joeri Toet is advocaat bij De Brauw, Blackstone Westbroek.

1. Zie art. 3:15d BW, de omzetting van Richtlijn 2000/31/EG inzake de elektronische handel maar het begrip diensten van de informatiemaatschappij is oorspronkelijk gedefinieerd in 1998: 'services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC'.
2. COM(2013) 48 final, 7.2.2013.
3. ENISA, *National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace*, May 2012, p. 9, zie ook H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, *Ten National Cyber Security Strategies: a comparison*, CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.

deren willen cybersecurity juist reserveren voor typische internetproblematiek. De discussie hierover zal blijven, aangezien 'cyber' weliswaar gebruikt wordt om internetfenomenen mee aan te duiden, maar de oorsprong niet internet gerelateerd is. De oude Grieken spraken van κυβερνητικός om goed bestuur mee aan te duiden, via informaticus Norbert Wiener die in de jaren veertig de term cybernetics gebruikte werd de term cyberspace (alsmede Matrix) gebruikt door science-fiction auteur William Gibson in de jaren tachtig en vervolgens met name in Amerikaanse (juridische) literatuur in de jaren negentig veelvuldig gebruikt om het internet mee aan te duiden.
Het lijkt ons zuiver om cybersecurity te omschrijven als een streven naar, of een staat van, bescherming tegen onrechtmatig verwerken van elektronische gegevens of onrechtmatig gebruik van computersystemen. Cybersecurity is geen doel op zich, maar veeleer een aspect van een kwalitatief hoogwaardige informatiehuishouding. Dat daar het een en ander aan schort en dat er werk gemaakt moet worden van het verbeteren daarvan lijkt breed gedragen te worden als we afgaan op de veelheid aan initiatieven wereldwijd.[4]

Maatschappelijk belang

De belangen bij een veilig internet zijn ontegenzeggelijk groot. Het is moeilijk voor te stellen hoe onze maatschappij zonder informatietechnologie zou functioneren. Eurostat becijferde in 2011 dat er ongeveer 380 miljoen internetgebruikers in de EU lidstaten zijn op een totaal van 500 miljoen inwoners. Nederland scoort met meer dan 80% internetpenetratie bovengemiddeld (tegen 76% binnen de EU).[5] Al in 2001 stelde de Europese Commissie vast dat een adequaat niveau van beveiliging van netwerk- en informatiesystemen van cruciaal belang is voor het functioneren van de Europese interne markt en onze maatschappij en richtte daarom in 2004 het Europese Netwerk- en Informatie Systemen Agentschap (hierna: ENISA) op:[6]

> 'Computers en netwerken groeien uit tot alomtegenwoordige nutsinstellingen (...) De beveiliging van communicatienetwerken en informatiesystemen, en in het bijzonder de beschikbaarheid ervan, is daarom van steeds groter belang voor de maatschappij (...) vanwege de mogelijkheid dat zich problemen voordoen in essentiële informatiesystemen (...) die gevolgen kunnen hebben voor de fysieke infrastructuur die diensten levert welke voor het welzijn van de EU-burgers van cruciaal belang zijn.'

Er wordt een duidelijke koppeling gelegd tussen de fysieke en elektronische infrastructuur. Het belang van de beschikbaarheid van de elektronische infrastructuur is in de loop der tijd toegenomen en dat geldt evenzeer voor de afhankelijkheid tussen de elektronische en fysieke infrastructuur.

Incidentpolitiek?

De aandacht voor het thema cybersecurity lijkt te worden gevoed door het grote aantal beveiligingsincidenten dat de laatste tijd in het nieuws komt. De Europese Commissie neemt als uitgangspunt voor haar laatste beleid dat cyberincidenten in aantal, omvang en complexiteit enorm toenemen:[7]

> 'Er zijn aanwijzingen dat grootschalige aanvallen op de informatiesystemen die vaak van vitaal belang kunnen zijn voor staten of voor specifieke onderdelen van de publieke of particuliere sector steeds gevaarlijker en fre-quenter worden.'[8]

De vraag is in hoeverre er van een toename in absolute zin sprake is. Niet uitgesloten is dat het beeld enigszins vertekend wordt door verbeterde waarneming van (pogingen) tot misbruik van gegevens of systemen en dat er een toenemende bereidheid of noodzaak ontstaat om te rapporteren over incidenten die zich hebben voorgedaan. Ook de oprekking van de definitie, of het hanteren van verschillende definities in verschillende soorten wetgeving draagt mogelijk bij aan de toename. Hoe het zij, tijdens de publieke consultatie op het laatste beleidsvoorstel van de Europese Commissie gaf 56,8% van de respondenten aan dat zij in het afgelopen jaar negatieve gevolgen heeft ervaren van incidenten betreffende netwerk- en informatiesystemen.[9] Gezien de afhankelijkheid van technologie lijkt ons dat voldoende reden tot zorg. De vraag is of en hoe daarop gepast zou kunnen worden ingegrepen.
Bij het overwegen van ingrijpen van overheidswege plaatsen wij een andere kanttekening. In het nieuws krijgen incidenten die (ogenschijnlijk) veroorzaakt zijn door moedwillig handelen verreweg de meeste aandacht. Gekeken naar de oorzaak van incidenten wordt daarbij vaak een onderscheid gemaakt naar de motieven van de betrokken actoren, zoals vandalisme, hacktivisme, cybercrime, spionage en elektronische oorlogsvoering. Minder vaak horen we over incidenten die het gevolg zijn van overmacht (bijv. natuurrampen) of onbedoeld handelen zoals onachtzaamheid van gebruikers, slecht systeem design of programmeerfouten of. Deze vormen evenwel een niet verwaarloosbare dreiging.[10] Het Ponomon Institute concludeert dat 64% van alle incidenten inzake data breaches toerekenbaar is aan menselijke fouten en

4. Niet alleen in Europa worden er initiatieven genomen om een hoger niveau van informatiebeveiliging te bereiken. Reeds in 2005 stond het onderwerp prominent op de agenda van de International Telecommunication Union (ITU, WSIS Thematic Meeting on Cybersecurity, Geneva, 10 June 2005 - http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf). Een meer recent voorbeeld is het initiatief van de Verenigde Staten van Amerika http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.
5. Eurostat, *Internet use in households and by individuals in 2011*, 8 december 2011.
6. Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging.
7. Europese Commissie, *EU oppert plan voor cyberbeveiliging: bescherming van open en vrij internet en kansen in digitale wereld*, 7 februari 2013.
8. Overweging 5 Richtlijn 2013/40 inzake aanvallen op informatiesystemen.
9. Europese Commissie, *Impact assessment accompanying proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union*, SWD(2013) 32 final, 7 februari 2013.
10. 'Storing bij Vodafone na brand in Rotterdam - voorlopig nog niet geblust, *NRC* 4 april 2012 en 'Ziggo verliest gegevens van veertigduizend klanten', *NRC* 12 oktober 2013.

systeemfouten.[11] Uit deze studie volgt dus dat de onderzochte incidenten in de meeste gevallen juist niet te wijten zijn aan het handelen van kwaadwillenden. Dit onderstreept ons inziens de opvatting dat het doel van eventueel juridische maatregelen niet zozeer gericht zou moeten zijn op beveiliging als zodanig, maar breder op het professionaliseren van technologie en het gebruik daarvan. In lijn met de gebruikelijke term Privacy by Design, kunnen we hiervoor het concept Cybersecurity by Design hanteren.[12]

Sociale en economische factoren

Hoewel techniek soms perfectie wordt toegedicht is net als bij veiligheid in het algemeen er nooit 100% garantie te geven. Zeker twee niet-technische aspecten spelen hierbij ook een rol.

Zo moet de menselijke factor niet uit het oog worden verloren. Het zogenaamde 'social engineering', waarbij iemand zich toegang tot bijvoorbeeld medische systemen verschaft door in een witte jas in een ziekenhuis rond te lopen en zich als arts voor te doen, vormt een belangrijke, niet technische dreiging. De beroemdste veroordeelde hacker, Condor, maakte bijvoorbeeld voornamelijk gebruik van deze niet technische handelswijze.[13]

Een maatschappelijk probleem komt tot stand door een complexe interactie tussen de participanten in die maatschappij en kwalificeert zich als er financiële belangen spelen als een economisch probleem. Het op effectieve wijze ingrijpen in de interactie tussen participanten in de maatschappij vereist dan een begrip van de economische processen die ten grondslag liggen aan het probleem. Dit geldt ook indien getracht wordt in te grijpen op (de totstandkoming van) gebrekkige beveiliging. Een aantal bijzondere economische processen liggen aan de totstandkoming en het in stand houden daarvan ten grondslag.

Een aspect dat genoemd moet worden is dat bedrijven geprikkeld kunnen worden tot, of zelfs belang kunnen hebben bij, de inzet van imperfecte informatietechnologie of meer algemeen bij beperkte of onvolledige beveiliging. Dit speelt ondermeer als bedrijven niet zelf de nadelen ondervinden:[14]

> 'Systems tend to fail when the people who defend them are not the people who suffer when they fail.'

Dit laat zich kwalificeren als de externalisering van kosten. Dit wordt versterkt indien de partijen die kosten kunnen externaliseren actief zijn op markten die gekenmerkt worden door economische netwerkeffecten. Deze effecten doen zich voor op markten waar de waarde van het product afhankelijk is van de omvang van de gebruikersbasis. Dat is bijvoorbeeld het geval bij veel hardware en software producten die volgens een bepaald protocol met elkaar communiceren. Voor bedrijven die dergelijke producten leveren bestaat er een sterke prikkel om een product zo snel mogelijk naar de markt te brengen omdat dan zo snel mogelijk een gebruikersbasis kan worden gecreëerd. Het is niet ongebruikelijk voor softwarebedrijven om eerst een onvolledige versie van een product op de markt te brengen en door de tijd te verbeteren door het uitbrengen van updates. Het laat zich raden dat in vroege versies van producten nog veel fouten zitten die al of niet door misbruik kunnen leiden tot incidenten. Het voordeel dat behaald kan worden door minder veilige systemen te ontwikkelen wordt kennelijk niet afgestraft door de schade die door deze gebreken geleden wordt.

Bestaande regelgeving

In verschillende Europese regelingen zijn al geruime tijd maatregelen aanwezig die een zeker niveau van beveiliging nastreven. Zo bevatten de Data Protectie Richtlijn en de ePrivacy Richtlijn generieke verplichtingen om informatie adequaat te beveiligen.[15] In de ePrivacy Richtlijn is met de laatste wijziging inmiddels ook een meldplicht voor inbraken op informatiesystemen opgenomen.[16] De begin 2012 voorgestelde Algemene Privacy Verordening bevat zelfs een sectie gewijd aan security (art. 30-32). Binnen de financiele sector moeten al langere tijd incidenten met mogelijke ontwrichtende effecten voor de integriteit van het financiële stelsel worden gemeld bij de toezichthouder.[17]

Op nationaal niveau zijn er verschillende wetten en regelingen die relevant zijn voor cybersecurity, we stippen ze slechts aan. Naast de beveiligings- en meldplichten zijn er ook informatieplichten in de verschillende sectorale wetten te vinden. Behalve deze bestuursrechtelijke regelgeving speelt tenslotte nog civiel recht (contractuele aansprakelijkheid, onrechtmatige daad) en strafrecht (santionering en opsporingsmethoden) een rol.

Nederlandse initiatieven

In de meeste EU lidstaten zijn nationale centra en cybersecurity strategieën ontwikkeld. In Nederland bestaat sinds 2012 het Nationale Cybersecurity Centrum (hierna: NCSC). Hoewel de naam NCSC anders doet vermoeden, zijn de bevoegdheden beperkt en toont de organisatorische inbedding duidelijk de sporen van competentiestrijd op hoog ambtelijk niveau. De missie klinkt dan ook weinig krachtdadig:

> 'Het NCSC draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief.'

Enerzijds leveren ze een inzicht en bieden een perspectief (adviesfunctie), anderzijds coördineren zij activiteiten om digitale weerbaarheid te vergroten. Kerntaken van het NCSC zijn:

1. Expertise opbouwen en advies geven
2. Respons op dreigingen en incidenten
3. Versterken van de crisisbeheersing

Het probleem bij crisisbeheersing op internet is dat bevoegdheden verspreid zijn over verschillende organisaties. Is een digitale dreiging van een crimineel, dan is de politie/OM aangewezen. Bij dreiging van een terrorist, de AIVD.

---

11. Ponemon Institute (gesponsored door Symantec), *2013 Cost of Data Breach Study: Global Analysis*, mei 2013.
12. Met dank aan Berend van der Eijk voor deze suggestie.
13. K.D. Mitnick & W.L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Wiley 2003.
14. T. Moore & R. Anderson (2011), *Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research*, TR-03-11, Computer Science Group, Harvard University.
15. Art. 17 Richtlijn 1995/46/EC en art. 4 2002/58/EC.
16. Richtlijn 2009/136/EC.
17. Voor een overzicht van meldplichten (gas, water, telecom, etc.) zie bijlagen bij brief van Minister van Veiligheid en Justitie van 6 juli 2012, *Kamerstukken* 26 643, nr. 247.

Bij dreiging van een andere staat, het leger. Voor daadwerkelijke slagkracht zouden deze competenties moeten samenkomen in het NCSC, te meer daar bij een dreiging op internet veelal niet duidelijk is wie er achter zit. Zover is het echter nog niet. De zogenaamde Emergency Response Teams (punt 2) zijn bijvoorbeeld deels overgegaan in NCSC (GovCert) en deels nog onderdeel van het leger (DefCert). Deze nationale competentieproblemen zullen ook op EU niveau niet eenvoudig kunnen worden weggenomen. Internationale samenwerking is echter noodzakelijk vanwege het grensoverschrijdende karakter van cybersecurity, reden waarom er vanuit de EU diverse initiatieven zijn.

EU-initiatieven

De bestaande maatregelen op Europees en nationaal niveau ten spijt stelde de Europese Commissie in 2013 vast dat het niveau van beveiliging dat onder de huidige omstandigheden bereikt wordt onvoldoende is. Zij acht belangen dermate groot en de dreiging zo evident dat nader ingrijpen noodzakelijk is. Begin 2013 publiceerde de Europese Commissie daarom een alomvattende cybersecurity strategie.[18] Een belangrijk onderdeel van deze strategie bestaat uit een Europese Richtlijn met maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de EU te waarborgen.[19]
Het grensoverschrijdende karakter van internet en de globaliserende samenleving zijn van invloed op cybersecurity, ziet ook de Europese Unie in:

> 'Vanwege dat transnationale karakter kan een ernstige verstoring van die systemen in een lidstaat ook andere lidstaten en de Unie als geheel treffen. De veerkracht en stabiliteit van netwerk- en informatiesystemen is daarom essentieel voor de soepele werking van de eengemaakte markt.'[20]

ENISA is zoals gezegd actief op het terrein van digitale veiligheid[21] en moet er op toezien dat binnen de EU problemen rond netwerkveiligheid worden voorkomen, beheerst en opgelost. Om dit te realiseren bevordert ENISA de samenwerking binnen de beveiligingsmarkt en wordt bijstand en advies verleend aan de EU alsmede de lidstaten. Kort na de oprichting van ENISA is in 2005 een kaderbesluit inzake aanvallen op informatiesystemen gepubliceerd dat ten doel had computercriminaliteit te bestrijden en de beveiliging van informatie te bevorderen.[22] In juni 2013 is een verordening gepubliceerd die ten doel heeft ENISA te moderniseren en versterken.[23]

Richtlijn inzake aanvallen tegen informatiesystemen

In 2010 is door de Europese Commissie een Richtlijn voorgesteld dat eerder genoemd kaderbesluit vervangt[24] om Europa beter te beschermen tegen cyberaanvallen.[25] Begin 2013 was deze richtlijn nog niet definitief vastgesteld en er wordt naar de nog lopende onderhandelingen daarover binnen de Europese Unie verwezen in het Richtlijnvoorstel inzake netwerk- en informatiebeveiliging.[26] Uiteindelijk is in de zomer van 2013 de richtlijn aanvallen tegen informatiesystemen definitief vastgesteld.[27]
Door middel van deze richtlijn wordt niet zozeer getracht in te grijpen op het niveau van informatiebeveiliging als wel om misbruik van kwetsbare technologie te voorkomen of te bestraffen.

De richtlijn bevat bepalingen over ondermeer onrechtmatige toegang (art. 3), systeemverstoring (art. 4) en gegevensverstoring (art. 5). De harmonisering van straffen blinkt niet uit in helderheid (art. 9 lid 1): 'doeltreffende, evenredige en afschrikkende straf-'. Daar kun je nog alle kanten mee op. Het strafminimum lijkt duidelijk (2 jaar, 3 jaar), maar kent de ambigue toevoeging 'althans voor gevallen die niet onbeduidend zijn.'
De inzet van het strafrecht zal in de praktijk vermoedelijk het meest effectief zijn tegen online vandalisten, hacktivisten en cybercriminelen. Vanwege de strafrechtelijke invalshoek zal het nagenoeg onmogelijk zijn om grip te krijgen op statelijke actoren. Een praktische beperking van de inzet van het strafrecht vloeit daarnaast voort uit de beperkte geografische werkingssfeer. Het zal bijvoorbeeld lastig zijn om georganiseerde misdaad in Rusland te bestrijden. De rechtsmachtbepaling (art. 12) is ook niet direct op het internet toegesneden: 'geheel of gedeeltelijk op hun grondgebied zijn gepleegd.' Wanneer is daar sprake van op internet?
Naast strafrechtelijke harmonisatie wordt ook samenwerking nagestreefd (art. 1):

> 'Zij strekt er tevens toe de preventie van deze strafbare feiten te vergemakkelijken en de samenwerking tussen de justitiële en de andere bevoegde autoriteiten te verbeteren.'

Deze samenwerking richt zich primair op informatieuitwisseling (art. 13):

> 'een operationeel nationaal contactpunt en gebruikmaken van het bestaande netwerk van operationele contactpunten die vierentwintig uur per dag en zeven dagen per week bereikbaar zijn'

18. Europese Commissie, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', JOIN(2013) 1 final, 7 februari 2013.
19. COM(2013) 48 final, 7 februari 2013.
20. Overweging 3 voorstel Richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, 7 februari 2013, COM(2013) 48 final.
21. Verordening 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, *PbEG* L77 13.03.2004, p. 1 -11.
22. Kaderbesluit 2005/222/JBZ over aanvallen op informatiesystemen, *PbEG* L69, 16.03.2005, p. 67-71.
23. Voorstel voor een Verordening Inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), 30.9.2010, COM(2010) 521 def.
24. Voorstel Richtlijn over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ, Brussel, 30.9.2010 COM(2010) 517 def.
25. Commissie wil Europa beter beschermen tegen cyberaanvallen, 30.09.2010, IP/10/1239.
26. Voorstel Richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen,. Over de verordening COM(2010) 521 def op p. 6, voetnoot 13. Over de Richtlijn COM(2010) 517 def. p. 6, voetnoot 19.
27. Richtlijn 2013/40/EU over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad, *PbEU* L 218/8, 14.08.2013.

Dit vereiste was ook terug te vinden in art. 35 van het Cybercrime verdrag,[28] maar de ervaring leert dat lang niet alle landen over een dergelijk altijd bereikbaar contactpunt beschikken. Mogelijk dat het Europese Cybercrime centrum, EC3, in dezen een belangrijke rol kan gaan spelen.

EC3: Europees Cybercrime Centrum

Onder de vlag van Europol is per 1 januari 2013 het Europese Cybercrime Centrum, EC3, begonnen, een in Den Haag gevestigde organisatie onder leiding van de Nederlander Troels Oerting. De drie aandachtsgebieden zijn aan internet gerelateerde fraude door georganiseerde misdaad en sexuele exploitatie van minderjarigen, en voor cybersecurity met name interessant de criminaliteit die kritische infrastructuur en informatiesystemen binnen de EU aantast.
De samenwerking die EC3 faciliteert is behalve analytisch ook operationeel. Een coördinerende rol die zich richt op het tegengaan van cybercrime. Duidelijk is dat het al gesignaleerde op internet lastig te maken onderscheid in dreigingen ook door EC3 niet integraal kan worden aangepakt. Door de focus op criminaliteitsbestrijding, kan niet worden opgetreden tegen acties van statelijke actoren of op overheid gerichte acties (defensie) en met veiligheid samenhangende dreigingen zoals terrorisme (veiligheidsdiensten).

Voorstel richtlijn Netwerk- en Informatiebeveiliging

Deze nieuwe Richtlijn Netwerk- en Informatiebeveiliging maakt onderdeel uit van het nieuwste EU-initiatief dat ook een strategie voor cybersecurity omvat. De richtlijn volgt op de constatering van de Europese Commissie dat er binnen de Europese Unie als geheel onvoldoende bescherming bestaat tegen netwerk- en informatiebeveiligingsincidenten, hetgeen het functioneren van de interne markt bedreigt.

Grondslag

De grondslag voor het richtlijnvoorstel is dan ook de interne markt (art. 26 en 114 VWEU). Het internet speelt een belangrijke rol bij het grensoverschrijdend verkeer van goederen, diensten en personen. Gezien het intrinsiek grensoverschrijdende karakter van het internet, kan verstoring van het verkeer in een lidstaat consequenties hebben in een andere lidstaat. Het internet is weliswaar een gedistribueerd netwerk waardoor uitval in een bepaalde lidstaat op zich niet gevolgen hoeft te hebben in een andere lidstaat, maar het verkeer met die andere lidstaat kan er wel door worden gehinderd alsmede is bij de tegenwoordig veel toegepaste clouddiensten het goed denkbaar dat informatie tijdelijk door lokale uitval elders ontoegankelijk wordt.
De oorzaak van dit probleem zoekt zij in de ongelijke capaciteiten van de lidstaten om op incidenten te kunnen reageren en de gebrekkige kennisdeling over dreigingen, risico's en incidenten in de Europese Unie.
Gesteld wordt dat het subsidiariteitsbeginsel een optreden van de EU op het gebied van Netwerk- en InformatieBeveiliging (zgn. NIB) rechtvaardigt. Het is weliswaar denkbaar dat zonder EU optreden iedere lidstaat maatregelen treft die vooral het eigen belang beschermen. Een bij (cyber)criminaliteit bijvoorbeeld bekend fenomeen is echter dat men door de zaken lokaal op te lossen het probleem verplaatst naar naastgelegen landen. Dit wil de EU bij internetdreigingen voorkomen. Samenwerking bij incidenten is geboden. Om die reden moeten de cybercapaciteiten en bevoegdheden van de lidstaten aansluiten. Ook verschillen in regelgeving die aan cybersecurity raakt moet worden weggenomen, zoals bijvoorbeeld in de hiervoor besproken Richtlijn 2013/40. Ook het evenredigheidbeginsel rechtvaardigt het richtlijnvoorstel: 'De NIB-vereisten waaraan de lidstaten moeten voldoen, worden vastgesteld op het minimale niveau dat vereist is voor een adequate paraatheid en een op vertrouwen gebaseerde samenwerking.'[29]

Doel

De richtlijn streeft er naar binnen de Europese Unie een hoger niveau van NIB te realiseren langs drie lijnen (Art. 1 lid 2 van Voorstel Richtlijn Informatiebeveiliging):[30]

1. De vaststelling van verplichtingen voor alle lidstaten met betrekking tot de preventie en behandeling van en de reactie op risico's en incidenten met betrekking tot netwerken en informatiesystemen;
2. De oprichting van een mechanisme voor samenwerking tussen de lidstaten met het oog op een uniforme toepassing van deze richtlijn in de Unie en, waar nodig, een gecoördineerde en doeltreffende behandeling van en reactie op risico's en incidenten met betrekking tot netwerken en informatiesystemen;
3. De vaststelling van beveiligingseisen voor marktdeelnemers en overheden.

Centraal uitgangspunt is dat de lidstaten moeten zorgdragen voor een veilig internet, vrij ruim omschreven in art. 4 als:

> 'waarborgen de lidstaten een hoog beveiligingsniveau van de netwerk- en informatiesystemen op hun grondgebied.'

Samenwerking

De voorgestelde richtlijn schept een kader waarbinnen de lidstaten moeten samenwerken om het niveau van informatiebeveiliging binnen de Europese Unie te verhogen. Deze richtlijn betrekt hierbij ook de private sector. Niet alleen overheidslichamen, maar ook als cruciaal aangemerkte categorieën van private partijen worden daarin betrokken. Daaronder worden behalve bepaalde dienstverleners van de informatiemaatschappij ook uitvoerders van kritieke infrastructuur die essentieel is voor het onderhoud van vitale economische en maatschappelijke activiteiten op het gebied van energie, transport, bankieren, beurzen en gezondheidszorg.[31] Deze partijen worden onderworpen aan een algemene verplichting om maatregelen te treffen tegen risico's voor de veiligheid van de netwerken en informatiesystemen die zij onder hun hoede hebben.[32] Zij moeten bovendien de toezichthoudende autoriteiten inlichten van incidenten die zich

28. *Trb.* 2002, nr. 18.
29. Voorstel, p. 10.
30. Voor een kritische kanttekening zie W. van Holst (2013), Richtlijn cybersecurity: Gemiste kans. Het voorstel van Kroes roept veel vragen op, *Automatiseringsgids* 7 mei 2013.
31. Art. 3(8) NIS-Richtlijn noemt (i) aanbieders van diensten van de informatiemaatschappij die het leveren van andere diensten van de informatiemaatschappij mogelijk maken en (ii) uitvoerders van kritieke infrastructuur die essentieel is voor het onderhoud van vitale economische en maatschappelijke activiteiten op het gebied van energie, transport, bankieren, beurzen en gezondheidszorg.
32. Art. 14(1) NIS-Richtlijn.

voordoen en die een aanzienlijke invloed hebben op de veiligheid van de kerndiensten die zij aanbieden.[33]

Meldplicht

De geïntroduceerde meldplicht voor incidenten richt zich tot een breed publiek. Dit kan om verschillende redenen waardevol zijn. In de eerste plaats is van belang te onderkennen dat investeringen in de kwaliteit van informatiesystemen en uitgaven aan beveiliging verantwoord moeten worden. Het risico bestaat altijd dat daarop te veel bezuinigd wordt. Als onder vigeur van een meldplicht de juiste informatie gedeeld wordt met de juiste partijen dan kan dit inzicht helpen om risico's in te schatten en om deze te 'beprijzen'. De kans dat risico's worden onderschat - zoals nu veelal het geval lijkt te zijn - neemt af.
In de tweede plaats kan de beoogde meldplicht helpen om het externaliseren van kosten te voorkomen of in ieder geval beperken. Transparantie helpt getroffen derden om schadebeperkende maatregelen te nemen tegen de gevolgen van incidenten en om schade te verhalen. Een meldplicht kan helpen om te voorkomen dat partijen die te weinig in hun informatiehuishouding en beveiliging investeren, de gevolgen daarvan op anderen kunnen afwentelen. Een belangrijke beperking van de waarde van de meldplicht lijkt evenwel te zijn gelegen in het feit dat hardware en software producenten daarvan uitgezonderd blijven.[34] De vraag is of daarmee niet ten onrechte een belangrijke bron van incidenten buiten beeld blijft.

Conclusie

Op Europees niveau wordt inmiddels met een breed palet van strafrechtelijke maatregelen, beveiligingsplichten en meldplichten getracht om een adequaat niveau van kwaliteit en beveiliging van de informatiehuishouding te waarborgen. De meeste maatregelen waren in eerste instantie voornamelijk gericht op actoren in selectief gekozen gebieden. We zien dat het bereik van deze maatregelen langzaam wordt uitgebreid. De komende jaren zullen moeten uitwijzen in hoeverre de Europese Unie succesvol in staat blijkt om hiermee binnen de gehele Europese Unie een veilig en betrouwbaar internet te garanderen. Hierbij is in de eerste plaats van belang dat niet volstaan wordt met het introduceren van meldplichten zonder dat goed wordt nagedacht over wat precies met de verschillende plichten bereikt wordt. Cruciaal is ook de samenwerking binnen de EU, want de vraag is of de nu bestaande ongelijkheid in de wijze waarop cybersecurity nationaal wordt aangepakt in voldoende mate op elkaar kan worden afgestemd. De competentieproblemen die we op nationaal niveau zien (leger, opsporing, veiligheidsdiensten) spelen zeker ook op internationale schaal. Er is dus nog een lange weg te gaan, maar over de eerste stappen zijn we voorzichtig optimistisch.

33. Art. 14(2) NIS-Richtlijn.
34. Overweging 24 NIS-Richtlijn.